Release Notes

7.2 and Updates

Copyright © 2008 Red Hat, Inc.

Copyright © 2008 Red Hat, Inc.. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later with the restrictions noted below (the latest version of the OPL is presently available at *http://www.opencontent.org/openpub/*).

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive
Raleigh, NC 27606-2072USAPhone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588Research Triangle Park, NC 27709USA

1. Introduction 2
2. New Features in Red Hat Certificate System 7.2 2
3. Deployment Notes 4
    3.1. Server Support 4
    3.2. Optional Server Hardware 5
    3.3. Client Support 6
    3.4. Optional Client Hardware 6
    3.5. Other Required Software 6
    3.6. Red Hat Enterprise Linux Considerations 6
    3.7. Sun Solaris Considerations 7
4. Obtaining Packages 7
5. Important Notes 8
    5.1. Installation Notes 8
    5.2. Required JRE 8
    5.3. Required JDK 9
    5.4. TPS Subsystem Considerations 10
    5.5. Directory Server Information 10
    5.6. Source RPMs 10

5.7. New File Locations and Subsystem URIs 10
6. Known Issues 11
7. Updates and Errata Releases for Red Hat Certificate System 7.2 16
8. Documentation 19
9. Copyright and Third-Party Acknowledgments 20
10. Document History 24

1. Introduction

These release notes contain important information available at the time of release for Red Hat Certificate System 7.2. New features, system requirements, installation notes, known problems, resources, and other current issues are addressed here. Read this document before beginning to use Red Hat Certificate System.

2. New Features in Red Hat Certificate System 7.2

Red Hat Certificate System 7.2 is a powerful public-key infrastructure (PKI) system containing the following new features:

- New silent installation script to ease installing and configuring multiple subsystem instances
- New security domain structure to organize and streamline communications between subsystems
- Enhanced cloning functionalities utilizing the new security domain organization
- Enhanced Red Hat Enterprise Security Client GUI and diagnostic and Phone Home functionality
- Multiple distinct packages rather than a single all-encompassing package
- A new standards-based architecture which more closely integrates Red Hat Certificate System with its base operating system
- Simplified browser-based HTML configuration panels for setting up subsystems
- Replaced Netscape Enterprise Server (NES) with Tomcat and Apache web servers
- Decoupled Red Hat Directory Server from Red Hat Certificate System
- Relocatable Red Hat Certificate System subsystem instances
- New supported server platform, Red Hat Enterprise Linux AS 4 (Intel 64-bit)
- New supported client platform, Apple Macintosh OS X 10.4.x (Tiger) (Power PC 32-bit)

Red Hat Certificate System 7.1 was comprised of a single large package. Red Hat Certificate System 7.2 has been modularized into numerous smaller packages to allow easier support by updating an existing package rather than the entire server. This has the additional advantage of allowing changes to be more easily tracked through the operating system's package management database. For example, 32-bit Red Hat Enterprise Linux 4 version of Certificate System is comprised of the following nine *entry-point* packages:

Package Name	Package Description
rhpki-ca-7.2.0-1.noarch.rpm	Certificate Authority (CA)
rhpki-kra-7.2.0-1.noarch.rpm	Data Recovery Manager (DRM); also known as Key Recovery Authority (KRA)
rhpki-ocsp-7.2.0-1.noarch.rpm	Online Certificate Status Protocol (OCSP) Responder
rhpki-tks-7.2.0-1.noarch.rpm	Token Key Service (TKS)
rhpki-tps-7.2.0-1.i386.rpm	Token Processing System (TPS)
rhpki-console-7.2.0-1.noarch.rpm	PKI Console
rhpki-java-tools-7.2.0-1.noarch.rpm	Java™-based command-line tools
rhpki-native-tools-7.2.0-1.i386.rpm	Native command-line tools
esc-1.0.0-16.i386.rpm	Red Hat Enterprise Security Client

Table 1. Packages in Red Hat Certificate System 7.2

The new modular architecture is based upon standards such as the Filesystem Hierarchy Standard (FHS) 2.3. This means that there is no longer an all-inclusive server root. Rather, Red Hat Certificate System server functionality is implemented through distribution to appropriate locations within the operating system. For example, 32-bit Red Hat Certificate System libraries are located under **`/usr/lib`**, binaries are located under **`/usr/bin`**, and Java™ archives (jars) are located under **`/usr/share/java`**.

In Red Hat Certificate System 7.1, the Java™-based tool **`startconsole`** was used to configure and manage any server instance of Red Hat Certificate System. In Red Hat Certificate System 7.2, an HTML-based configuration wizard is used to configure any new subsystem instance, while a utility called **`pkiconsole`** is used to manage existing instances. The HTML configuration panels are individually customized for subsystem type.

Red Hat Certificate System 7.1 used Netscape Enterprise Server as an integrated web server for all of its HTTP/HTTPS transactions. Red Hat Fortitude provides a Network Security Services (NSS) module to the Apache HTTP Server 2.0 and a Java™ Security Services (JSS) plug-in to Tomcat 5.5. The legacy NES web server in CA, DRM, OCSP, and TKS subsystems has been replaced by Tomcat running Fortitude, and the legacy NES web server in TPS subsystems has been replaced by Apache running Fortitude.

Previously, Red Hat Directory Server was bundled and installed with Red Hat Certificate System. Red Hat Certificate System 7.2 still requires a Red Hat Directory Server 7.1 (SP 3) installation for each subsystem at configuration, but this server must be installed separately and before the Certificate System is installed.

NOTE

The Red Hat Directory Server can be installed on a separate machine, which is the recommended scenario for most production deployments.

Red Hat Certificate System 7.2 creates and removes instances of CA, DRM, OCSP, TKS, and TPS through command-line utilities called **pkicreate** and **pkiremove**. The **pkicreate** utility allows an instance to be placed anywhere on the operating system, including a data partition that may be RAID-enabled. This allows true separation of unique Red Hat Certificate System data from shared Red Hat Certificate System libraries, executables, and jars, thus providing a better means of maintaining the security and integrity of a user's valuable data. Furthermore, a Red Hat Certificate System instance may only be removed by running **pkiremove**; removing the core Red Hat Certificate System services have no effect on any Red Hat Certificate System instances installed on a given system.

The Red Hat Certificate System 7.2 server product is now available for 64-bit Red Hat Enterprise Linux 4 (AMD64 and Intel EM64T) platforms, as well as 32-bit Red Hat Enterprise Linux 4 (i386).

Red Hat Enterprise Security Client 1.0 is now available on Apple Macintosh OS X 10.4.x (Tiger), as well as Microsoft Windows XP Professional and 32-bit and 64-bit Red Hat Enterprise Linux 4. The TokenD implementation in the new Enterprise Security Client allows use of Red Hat Certificate System smart card technology to be integrated with Apple applications such as the Safari Web browser and Apple Mail.

The Red Hat Enterprise Security Client GUI has been completely revamped and standardized across all platforms. Enhanced diagnostic information has been added to the UI. New Phone Home configuration streamlines the communication between the TPS and Enterprise Security Client and simplifies the initial Enterprise Security Client configuration.

3. Deployment Notes

This section contains information related to installing Red Hat Certificate System 7.2, including hardware and platform requirements and prerequisites.

3.1. Server Support

The Certificate System subsystems are supported on the following platforms:

- Red Hat Enterprise Linux AS 4 for i386
- Red Hat Enterprise Linux ES 4 for i386
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T
- 64-bit Solaris 9 for SPARC

Component	Details
CPU	Intel — 2.0 GHz Pentium 4 or faster
RAM	1 GB (required)

Hard disk storage space	Total is approximately 5 GB
	• Total transient space required during installation: 1 GB
	• Hard disk storage space required for installation:
	  • Space required to set up, configure, and run the server: approximately 2 GB
	  • Additional space for database growth in pilot deployment: approximately 1 GB
	  • Total disk storage space for installation: approximately 1 GB

Table 2. Server Requirements

3.2. Optional Server Hardware

- Chrysalis-ITS LunaSA Hardware Security Module (HSM)
  - Firmware: 4.5.2
  - Appliance Software: 3.2.4
  - Client Software: 3.2.4
- nCipher netHSM
  - Firmware: 2.12
  - Software: 9.01

3.3. Client Support

The Enterprise Security Client is supported on the following platforms:

- Apple Macintosh OS X 10.4.x (Tiger) (Power PC, Intel)
- Microsoft Windows XP Professional (i386)
- Red Hat Enterprise Linux AS 4 (i386)
- Red Hat Enterprise Linux ES 4 (i386)
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T

3.4. Optional Client Hardware

- Axalto Global Platform compatible Cyberflex eGate token

3.5. Other Required Software

- Red Hat Directory Server 7.1; the source code and binaries for this component are available at *https://1rhn.redhat.com*), through the Red Hat Directory Server 7.1 channel.
- Web browser software that supports SSL. It is strongly recommended that users such as agents or administrators use Mozilla Firefox. End-entities should use Mozilla Firefox or Microsoft Internet Explorer.

  The only browser that is fully-supported for the HTML-based instance configuration wizard is Mozilla Firefox.

3.6. Red Hat Enterprise Linux Considerations

Before installing the Certificate System packages, ensure that the proper dependencies are installed on the Red Hat Enterprise Linux system.

The following package groups and packages must be installed on all Red Hat Enterprise Linux systems:

- dialup (package group)

- gnome-desktop (package group)
- compat-arch-support (package group)
- web-server (package group)
- kernel-smp (package)
- e2fsprogs (package)
- firefox (package)

On 64-bit Red Hat Enterprise Linux platforms, ensure that the 64-bit (x86_64) **compat-libstdc++** libraries are installed, and not only the 32-bit (i386) libraries. To confirm this, run the following command as **root**:

```
rpm -qa --queryformat 'compat-libstdc++-%{VERSION}-%{RELEASE}.%{ARCH}.rpm
| grep x86_64
```

Numerous libraries should be displayed.

3.7. Sun Solaris Considerations

The Sun Solaris version of Certificate System was tested on Solaris 9 with patch level 118558-28.

4. Obtaining Packages

Red Hat Network (*http://1rhn.redhat.com*) is the software distribution mechanism for most Red Hat customers. Account login information for Red Hat Network, including entitlements for the Red Hat Certificate System 7.2 release, is required to download this software from Red Hat Network. After logging into Red Hat Network, go to the appropriate Red Hat Certificate System 7.2 channel to download the packages for the selected Red Hat Enterprise Linux platform.

NOTE

The source code for Red Hat Directory Server 7.1 is included with the ISO image downloaded for the 32-bit Red Hat Enterprise Linux version. Red Hat Certificate System itself is not yet open source.

Red Hat Enterprise Linux systems can upgrade or download Red Hat Certificate System using **up2date**.

5. Important Notes

The following sections contain important installation, configuration, and deployment information for Red Hat Certificate System 7.2.

5.1. Installation Notes

- Packages are non-relocatable. The Red Hat Certificate System base packages can not be installed to a user-designated location.

- Do not use the Autorun feature of the CD drive. If you use the Autorun feature with a CD created from the ISO image, all subsystems (CA, DRM, OCSP, TKS, and TPS) as well as the Enterprise Security Client are installed on the system by default.

  The preferred alternative is to run the installation scripts provided for the server, or to follow the installation instructions in the *Red Hat Certificate System 7.2 Administration Guide*.

5.2. Required JRE

Java™ 1.5.0 Java Runtime Environment (JRE). Certificate System does not support earlier versions of the JRE. This JRE is required for running Tomcat, among other applications for the Certificate System.

On 32-bit Red Hat Enterprise Linux 4 platforms, Certificate System 7.2 requires the 32-bit version of the IBM JRE 1.5.0. A pre-packaged binary distribution of this package, **`java-1.5.0-ibm-1.5.0.0-1jpp_2rh:0.i386`**, is available through either the **Red Hat Enterprise Linux AS (v. 4 for x86) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for x86) Extras** Red Hat Network channel.

Similarly, for 64-bit Red Hat Enterprise Linux 4 platforms, Certificate System 7.2 requires the 64-bit version of the IBM JRE 1.5.0. A pre-packaged binary distribution of this package, **`java-1.5.0-ibm-1.5.0.0-1jpp_2rh:0.x86_64`**, is available through either the **Red Hat Enterprise Linux AS (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel.

As **`root`**, run **`/usr/sbin/alternatives --config java`** to ensure that the IBM Java™ 1.5.0 JRE is selected.

Warning

Both the 32-bit xSeries (Intel-compatible) and 64-bit AMD/Opteron/EM64T versions of the IBM J2SE JRE 5.0 RPM packages available through the IBM download site are packaged in a format which is incompatible with Certificate System 7.2.

For 64-bit Solaris 9 (SPARC) platforms, download and install the latest version of the 64-bit Sun J2SE Java™ Runtime Environment 5.0 (Update 8) available from the Sun download site, *http://java.sun.com/javase/downloads/index.jsp*.

IMPORTANT

The 64-bit Solaris version of the Certificate System requires the user to install the 32-bit version of the JRE *as well as* installing the 64-bit version. The 32-bit version is used for the applet and Java™ Web Start support. Read *http://java.sun.com/j2se/1.5.0/README.html*, *http://java.sun.com/j2se/1.5.0/ReleaseNotes.html*, and *http://java.sun.com/j2se/1.5.0/jre/install-solaris-64.html* before installing the Certificate System.

Under the section *Java Runtime Environment (JRE) 5.0 Update 9*, Sun only makes this JRE available through a self-extracting file which is incompatible with Certificate System since this format does not use the native Solaris packaging utility database.

It is possible to obtain the Sun 5.0 JRE in a compatible format. Click **Download** under the JDK 5.0 Update 9 section, and, under **`Solaris SPARC Platform - J2SETM Development Kit 5.0 Update 9`**, select **`Solaris SPARC 32-bit packages - tar.Z (jdk-1_5_0_09-solaris-sparc.tar.Z)`** and **`Solaris SPARC 64-bit packages - tar.Z (use 32-bit version for applet and Java Web Start support) (jdk-1_5_0_09-solaris-sparcv9.tar.Z)`**.

After downloading these two files, uncompress them using the **`gunzip`** utility, and extract the contents using the **`tar`** utility.

The contents of the 32-bit file, **`jdk-1_5_0_09-solaris-sparc.tar.Z`**, are **`COPYRIGHT`**, **`LICENSE`**, **`README.html`**, **`SUNWj5cfg`**, **`SUNWj5dev`**, **`SUNWj5dmo`**, **`SUNWj5jmp`**, **`SUNWj5man`**, and **`SUNWj5rt`**.

The contents of the 64-bit file, **`jdk-1_5_0_09-solaris-sparcv9.tar.Z`**, are **`SUNWj5dmx`**, **`SUNWj5dvx`**, and **`SUNWj5rtx`**.

Since only the JRE is needed on Solaris 9 systems, use the **`pkgadd`** utility to add the 32-bit package, **`SUNWj5rt`**, first, and then add the 64-bit package, **`SUNWj5rtx`**.

5.3. Required JDK

A JDK must be present on Red Hat Enterprise Linux systems. See *http://kbase.redhat.com/faq/FAQ_54_4667.shtm* for more information. While almost any JDK is sufficient, installing one of these JDKs is recommended:

- For 32-bit Red Hat Enterprise Linux 4 platforms, a pre-packaged binary distribution of the 32-bit version of the IBM JDK 1.5.0, **`java-1.5.0-ibm-devel-1.5.0.0-1jpp_2rh:0.i386`**, is available through either the **Red Hat Enterprise Linux AS (v. 4 for x86) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for x86) Extras** Red Hat Network channel.

- For 64-bit Red Hat Enterprise Linux 4 platforms, a pre-packaged binary distribution of the 64-bit version of the IBM JDK 1.5.0, **`java-1.5.0-ibm-devel-1.5.0.0-1jpp_2rh:0.x86_64`**, is available through either the **Red Hat Enterprise Linux AS (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel.

After installing the JDK, run **`/usr/sbin/alternatives --config javac`** as **`root`** to insure that a JDK is available.

Solaris 9 systems do not require downloading and installing a JDK; however, it may be required to download and install the Sun JDK 5.0 package in order to obtain a compatible Sun JRE 5.0 package.

5.4. TPS Subsystem Considerations

- TPS subsystems installed on a Red Hat Enterprise Linux system require a local installation of the Apache 2.0.x web server. If the installation is made on a newly-installed Red Hat Enterprise Linux AS or ES system, rather than an upgraded system, and **Everything** was selected during the Anaconda installation process, an Apache server should already be present.

  When installing the TPS subsystem on Solaris 9, a specially-configured Apache server is included as part of the Certificate System 7.2 packages.

- The TPS subsystem cannot be cloned.

5.5. Directory Server Information

All subsystems require access to Red Hat Directory Server 7.1 on either the local machine (if it is also a 32-bit Red Hat Enterprise Linux platform) or a remote machine (acceptable platforms are 32-bit Red Hat Enterprise Linux 4, 32-bit Solaris 9 for SPARC, or 64-bit Solaris 9 for SPARC).

5.6. Source RPMs

Since Red Hat Certificate System 7.2 is not an open-source product, source RPMs are only available for third-party packages.

NOTE

Several of these third-party packages may issue warnings when they are installed because they may contain the UID or GUID of their original packager.

5.7. New File Locations and Subsystem URIs

The subsystem files in Certificate System 7.2 are in different locations than in Certificate System 7.1. The old and new locations are listed in *Table 3, "Certificate System 7.1 and 7.2 File Locations"*. These are explained in more detail in chapter 3, "Administrative Basics," in the *Certificate System Administrator's Guide*.

File	7.1 Location	7.2 Location
Subsystem start and stop scripts	**`/opt/redhat-cs/cert-`***instance_ID*	**`/etc/init.d/`***instance_ID*

File	7.1 Location	7.2 Location
Subsystem installation directory (default)	**/opt/redhat-cs/cert-***instance_ID*	**/var/lib/***instance_ID*
Subsystem configuration directory (default)	**/opt/redhat-cs/cert-***instance_ID***/config**	**/var/lib/***instance_ID***/conf**
Subsystem log files	**/opt/redhat-cs/cert-***instance_ID***/logs**	**/var/log/***instance_ID*
Tools	**/opt/redhat-cs/bin/cert/tools**	**/usr/bin**
Security databases	**/opt/redhat-cs/alias**	**/var/lib/***instance_ID***/alias**

Table 3. Certificate System 7.1 and 7.2 File Locations

In addition to differences between the default directories, versions 7.1 and 7.2 use different URLs for accessing the services HTML pages. The old and new locations are listed in *Table 4, "Certificate System 7.1 and 7.2 URLs"*.

Page	7.1 URL	7.2 URL
CA Services Page	**https://***hostname:SSLport*	**https://***hostname:SSLport***/ca/services**
CA Agents Page		**https://***hostname:SSLport***/ca/agent/ca**
CA End-Entities Page		**https://***hostname:SSLport***/ca/ee/ca**
DRM Services Page	**https://***hostname:SSLport*	**https://***hostname:SSLport***/kra/services**
DRM Agents Page		**https://***hostname:SSLport***/kra/agent/kra**
OCSP Services Page	**https://***hostname:SSLport*	**https://***hostname:SSLport***/ocsp/services**
OCSP Agents Page		**https://***hostname:SSLport***/ocsp/agent/ocsp**

Table 4. Certificate System 7.1 and 7.2 URLs

6. Known Issues

Table 5, "Known issues in Red Hat Certificate System 7.2" lists the known issues and supported workarounds in Red Hat Certificate System 7.2.

Bug Number	Description
57434	On Red Hat Enterprise Linux, a new CA server will not start after configuration if a SafeNet LunaSA 3.1 hardware module is used with SHA-512 as the CA signing algorithm. The CA server returns an error that the signature on the server certificate is

Bug Number	Description
	bad. SHA-256 can be used as the signing algorithm instead.

57514	If a TKS master key is generated on a SafeNet LunaSA HSM, server-side key generation fails with the following error in the TKS debug log:
	
	`"can't generate key encryption key"`
	
	A similar message also appears in the debug log if server-side key generation is turned on:
	
	`"TokenServlet: key encryption key generation failed for CUID"`
	
	where *CUID* is the card unique ID.

57526	If a server certificate contains the Authority Information Access extension, the certificate cannot be imported on an nCipher netHSM hardware token. The default caServerCert profile has this extension enabled by default. For example, when installing a subsystem such as the Token Key Service (TKS), the SSL server certificate fails to import if the certificate is processed through the default caServerCert profile because the caServerCert profile adds the Authority Information Access extension to the SSL server certificate automatically. If a CA server is already installed on the nCipher netHSM token, then the CA signing certificate is overwritten, as well. To import the server certificate properly, first remove the Authority Information Access extension from the caServerCert profile, then install the subsystem.
57677	If the DRM response to the TPS exceeds the timeout period, the server can return the incorrect response message, **`200 HTTP/1.1 OK`**, signaling that the operation completed successfully instead of timing out.
57640	If a DRM version 6.1 SP4 is migrated to version 7.2, then the archived keys that were migrated cannot be recovered because the key splitting schemes are different. To be able to recover these keys, first obtain a migration patch from Red Hat services. This patch will recover the PIN needed to access the storage token where the DRM private key resides, then recover the keys and export them to a PKCS #12 file. However, this package can potentially expose security issues in the version 6.1 SP 4 DRM, so it should be used only as necessary. For information on using these migration scripts, see the README available with the migration package.
57683	If there are multiple enrollment operations using the **`tpsclient`** tool when server-side key generation is enabled in the TPS, then the DRM connection can time out before the TPS can generate the keys. The tool will then return the error **`Failed to generate key on server. Please check DRM.`** To correct this, edit the TPS **`CS.cfg`** configuration file and add a line increasing the timeout period for the connection to the DRM: `conn.drm1.timeout=25`

Bug Number	Description
57800	It is possible for inconsistencies to arise between the TPS database and the CA database, so that certificate statuses may not be correct. The TPS database only maintains the certificate statuses on tokens that were last seen by the TPS system. For example, if a certificate is manually revoked by the CA agent, then that revocation status does not get updated automatically in the TPS database. There is no known workaround for this issue at this time.

57875	To verify if the full CA chain is in a security database, such as an OCSP or subordinate CA, open the security database directory, like **`/var/lib/instance_ID/alias`**.
	
	To list all the CA certificates and their nicknames, run **`certutil`** with the following options:
	
	`certutil -d . -L`
	
	To confirm that a particular certificate is included in the database, run **`certutil`** with the following options:
	
	`certutil -d . -L -n nickname`
	
	nickname is the nickname of the certificate.
	
	The only time a certificate chain is needed for the OCSP service is if the CA connects to the OCSP through SSL authentication when it publishes its CRL. Otherwise, the OCSP does not need to have the complete certificate chain to verify the CRL; the OCSP must have the certificate which signed the CRL, either the CA signing certificate or a CRL signing certificate. If both a root CA and one of its subordinate CAs publish CRLs to an OCSP, the OCSP needs the CA signing certificate of both CAs.
	
	The signing certificate can be imported into the OCSP database through the OCSP agent interface.

57978	Trying to add the **`nsTokenUserKeySubjectName`** default with **`No Constraint`** extension to a certificate profile through the Certificate Manager Console throws a null pointer exception, and the default is not added.
57991	The server certificate nicknames created through the subsystem configuration wizard cannot be edited in the Requests and Certificates panel. These certificate nicknames are not currently shown in that part of the configuration UI; that field is left blank in the pretty-print view. This can cause naming collisions if a hardware token is used for a subsystem and server certificates are already stored on the token.
58058	Generating key pairs on Safenet LunaSA hardware modules can fail with the error **`CKR_MAX_OBJECT_COUNT_EXCEEDED`**. On LunaSA tokens, the number of objects cannot exceed 127. When an object is deleted, the label for that object remains and is counted. Delete the empty labels to lower the count. Key generation can then proceed.
58201	When configuring a cloned CA, the administrator certificate panel is displayed, but grayed out. Clicking **Next** to proceed to the next panel displays a pop-up box that the certificate was successfully imported into the browser when, actually, no action was taken.
58228	Even after the configuration process is successfully completed, the configuration wizard

Bug Number	Description
	page can still be accessed. This page can be disabled by removing the **preop.pin** parameter from the instance's **CS.cfg** file and restarting the instance.
58301	Using the administrative console to renew an SSL server certificate stored on a hardware token automatically imports the server certificate into the Certificate System software token rather than the hardware token.
58354	It is possible for a CA, DRM, OCSP, and TKS subsystem's certificates to be generated by an external root CA. For a subordinate CA in that case, the new CA signing certificate issued by the external CA must be pasted into the Requests and Certificates page; this signing certificate is then used to generate the other certificates. For DRM, OCSP, and TKS subsystems, the SSL server and client certificates and, if required, DRM transport and storage certificates are generated by the external CA. It can take several days, even weeks, to receive the certificates from the external root CA, meaning the the configuration process is suspended at the Requests and Certificates panel in the configuration wizard. When the certificates are received, they must be pasted into the Requests and Certificates panel to complete the subsystem configuration. However, reopening the configuration wizard at the beginning of the process can corrupt the previous setup. To return directly to the Requests and Certificates panel in the configuration wizard, open the configuration wizard URL with **?p=12** appended to the end. For example: `http://server.example.com:9080/ca/admin/ console/config/wizard?p=12`
58464	On Mozilla Firefox, when accessing a subsystem URL without specifying the desired page, such as **https://server.example.com:9443**, it automatically redirects to **https://server.example.com:9443/ca/services**. The redirect does not work on Internet Explorer 6.0; when trying the URL **https://server.example.com:9443**, Internet Explorer opens a blank page.
58518	When starting or stopping a CA, DRM, OCSP, or TKS on Solaris, the start and stop script can kill the process before the process completes and exits. This does not occur on a TPS subsystem on Solaris.
58524	Before reusing an HSM to install and configure a TPS subsystem, manually delete any existing certificates from the HSM. All conflicting certificates (certificates with the same nickname) have to be removed from the HSM before the TPS is configured. Otherwise, the configuration process will still install the new certificates, but it is not certain which certificate, old or new, will be used. Running **certutil** with the **-D** option to delete the certificates does not work with the **-f** option to specify a password file.
58555	Safenet LunaSA hardware modules do not have binaries for 64-bit Red Hat Enterprise Linux platforms. Trying to use LunaSA 32-bit libraries on 64-bit Red Hat Enterprise Linux platforms, including Red Hat Enterprise Linux 4 (x86_64), will fail with the following error: `ERROR: Failed to add module "lunasa". Probable cause: "/ usr/lunasa/lib/libCryptoki2.so: cannot open shared object file: No such file or directory"`
58577	Agent authentication to an ECC-enabled CA can fail in the browser with error **-12271** if an HSM has been added to the **secmod.db** database on the local machine. To work around this situation, delete the **secmod.db** database which contains the HSM entry

Bug Number	Description
	and create a new **secmod.db** database.
58745	If two TPS instances are running on the same machine, stopping or restarting one instance will automatically restart the other instance. It is recommended that only one TPS instance run per machine.
58759	There are exception errors when trying to install a renewed certificate in the subsystem certificate database through the administrative console. Instead of using the Console to install renewed subsystem certificates, use the **certutil** utility.
58761	The HTML-based instance configuration wizard is only supported on Mozilla Firefox. Using an unsupported browser can result in incorrect behavior. For example, in Microsoft Explorer, the pretty-print certificates and the certificate requests are displayed on a single line.
58764	When setting up a clone, the Certificate System clone instance may record errors concerning the **ancestorid** attribute in the error log: `[30/Oct/2006:11:04:00 -0800] - warning: ancestorid not indexed on 21` `[30/Oct/2006:11:04:00 -0800] - warning: ancestorid not indexed on 21` `[30/Oct/2006:11:04:00 -0800] - warning: ancestorid not indexed on 21` These warnings can be ignored because they only indicate that the request repository is empty at the time the clone is configured; they do not indicate a problem with the clone instance.
58773	If a subsystem within a security domain needs to be re-installed, there may be a subsystem user already created in the security domain CA's user database if the previous installation was either successfully completed or stopped after the security domain was selected. Since the user names are created based on the hostname and port number, if the same port number is reused, the pre-existing entry prevents the next installation from inserting its subsystem certificate into the subsystem user's entry in the security domain. This causes the instance to fail to start because the authentication to the security domain fails. This can happen on any subsystem which is reinstalled, except for the security domain CA itself. To reinstall a subsystem without encountering these authentication errors, do the following: 1. When installation is aborted - or when completed, but it needs redone - remove the instance. For example: `pkiremove -pki_instance_root=/var/lib -pki_instance_name=rhpki-tps` 2. Open the Console for the security domain CA, and remove the subsystem user from the security domain CA user database:

Bug Number	Description

	``
	pkiconsole https://server.example.com:9443/ca/
	``
	a. Click on **Users and Groups** in the left navigation tree.
	b. Click on the subsystem user name, such as **`TPS-server.example.com-7889`**.
	c. Click **Delete**.
	3. Recreate the subsystem.
	``
	pkicreate -config_dir=/var/lib -subsystem_type=tps
	          -pki_instance_name=rhpki-tps
	          -secure_port=7888 -unsecure_port=7889
	          -user=pkiuser -group=pkigroup -verbose
	``
	4. Go through the configuration wizard again. The instance will restart successfully when the configuration is finished.

58779	When an nCipher HSM is used for a Certificate System instance, the **`nfast`** group needs to include the user ID of the Certificate System instance process. For example, since default Certificate System instances run as **`pkiuser`**, then the **`pkiuser`** group needs to be added as a member to the **`nfast`** group, if the Certificate System group has not already been added.
213805	If a token is plugged in when the Enterprise Security Client is installed, then the client can fail to recognize the token. To be certain that the Enterprise Security Client will recognize tokens, make sure that no smart card tokens are plugged in when the Enterprise Security Client packages are installed.
	Certificates cannot be installed or renewed in the certificate database through the Certificate Setup Wizard in the administrative console in Certificate System 7.2. The **`certutil`** utility can be used to manage certificates instead.

Table 5. Known issues in Red Hat Certificate System 7.2

7. Updates and Errata Releases for Red Hat Certificate System 7.2

The following erratas have been issued for Red Hat Certificate System, fixing important security and performance issues. The complete list of erratas issued for Red Hat Certificate System 7.2 is available through Red Hat Network for *Red Hat Enterprise Linux 4*[1].

[1] https://rhn.redhat.com/errata/rhel-certserv-72-errata.html

Release Date	Errata Release	Bug Number	Description
January 14, 2009	RHSA 2009:0006	249923 451998 (CVE 2008-2367) 452071	Red Hat Certificate System used insecure default file permissions on certain configuration files, such as **`password.conf`**, that may contain administrative passwords or other credentials. A local user could use that information to gain access to sensitive information stored in Certificate System subsystems.
		224732 451200 (CVE 2008-2368)	Red Hat Certificate System stored plain text passwords in multiple log files, such as some certificate profile logs and installation logs, which had insufficient access restrictions to prevent unauthorized users from viewing them. A local user could access the plain text password to gain access to Certificate System information.
		224904	Due to a regression, signing a certificate revocation list (CRL) with approximately 150,000 records may have taken up to five minutes. In these updated packages, signing such CRLs takes approximately twenty seconds.
		238514 306091	An OCSP client submitting an OCSP request via the GET method may have caused a NullPointerException. This errata adds support for processing OCSP requests submitted through a GET method.
		239876 308161	Because Certificate System subsystems could not handling Online Certificate Status Protocol (OCSP) requests in the GET method, OCSP GET requests resulted in a 404 error. This was also related to a problem which caused the subsystem to use 100% CPU when processing OCSP requests.
		243939	OCSP requests are now logged to the debug log file.
		243804 451726	When a new certificate revocation list (CRL) was being generated, new revocation requests were processed but not properly added to the CRL. This meant that certificates with higher serial numbers (i.e., more recent certificates) were not listed in the CRL and were not shown as revoked until the next CRL was generated. A user who had a revoked but otherwise valid certificate could take advantage of this issue to bypass the revocation list.
		243807	Inefficient LDAP search methods caused LDAP searches for 100,000 or more revoked certificates to take twenty minutes or longer during CRL generation. The LDAP search method has been modified to greatly improve

Release Date	Errata Release	Bug Number	Description
			LDAP search times.
		249229	The default OCSP verification path has changed since Red Hat Certificate System 7.1. These updated packages add support for certificates that use the old AuthorityInfoAccess URL.
		254232 330261	If an agent automatically approved a certificate signing request (CSR) using AgentCertAuth, the iisued certificate contained blank subjectAltName extension fields. A manual enrollment by the same agent produced a certificate with the correct number of subjectAltName fields, with no blank fields. This errata fixed automated enrollements using the AgentCertAuth profile so that the issued certificates do not have any blank fields.
		462143	The initial authentication to a security domain failed during subsystem configuration.
		462145	After its initial configuration, the TPS subsystem failed to restart.
July 2, 2008	RHSA 2008:0577	440356 442963 445227 445231 CVE-2008-1676	A flaw was found in the way Certificate System handled extensions in the certificate signing requests (CSR). All requested extensions were added to the issued certificate even if constraints were defined in the certificate authority (CA) profile. An attacker could submit a CSR for a subordinate CA certificate, even if the CA configuration prohibited subordinate CA certificates. This led to a bypass of the intended security policy, possibly simplifying man-in-the-middle attacks against users that trust Certificate System CAs.
January 9, 2008	RHBA 2000:0035	330261	If an agent automatically approved a certificate signing request (CSR) using AgentCertAuth, the iisued certificate contained blank subjectAltName extension fields. A manual enrollment by the same agent produced a certificate with the correct number of subjectAltName fields, with no blank fields. This errata fixed automated enrollements using the AgentCertAuth profile so that the issued certificates do not have any blank fields.
October 8, 2008	RHSA 2007:0934	224904 243176 243804 243807 304571 (CVE 2007:4994)	When a new certificate revocation list (CRL) was being generated, new revocation requests were processed but not properly added to the CRL. This meant that certificates with higher serial numbers (i.e., more recent certificates) were not listed in the CRL and were not shown as revoked until the next CRL was generated.

Release Date	Errata Release	Bug Number	Description
			A user who had a revoked but otherwise valid certificate could take advantage of this issue to bypass the revocation list.
		308161	If Certificate System received an OCSP request using the GET method, it returned an HTTP 404 error because it could not properly handle GET requests.
September 24, 2007	RHBA 2007:0927	254232	This extracts extensions from PKCS#10 requests to use within the profile framework.

Table 6. Bugs Fixed in Errata Updates for Certificate System 7.2

8. Documentation

The *Certificate System Administrator's Guide* describes how to set up, configure, and administer the Certificate System subsystems and how to configure backend certificate management functions, such as publishing and logging. The *Administrator's Guide* also describes how to configure subsystems to relate to one another to manage certificates and tokens and how to manage certificates and tokens; this guide is targeted for Certificate System administrators.

The *Certificate System Agent's Guide* describes how agents — users responsible for processing certificate requests and managing other aspects of certificate management — can use the Certificate System subsystems web services pages to process certificate requests, key recovery, OCSP requests and CRLs, and other functions.

The documentation for Certificate System includes the following guides:

- *Certificate System Administrator's Guide* explains all administrative functions for the Certificate System, such as adding users, creating and renewing certificates, managing smart cards, publishing CRLs, and modifying subsystem settings like port numbers.

- *Certificate System Agent's Guide* details how to perform agent operations for the CA, RA, DRM, and TPS subsystems through the Certificate System agent services interfaces.

- *Certificate System Command-Line Tools Guide* covers the command-line scripts supplied with Red Hat Certificate System.

- *Managing Smart Cards with the Enterprise Security Client* explains how to install, configure, and use the Enterprise Security Client, the user client application for managing smart cards, user certificates, and user keys.

- *Certificate System Migration Guides* cover version-specific procedures for migrating from older versions of Certificate System to Red Hat Certificate System 7.2.

- *Release Notes* contains important information on new features, fixed bugs, known issues and work-

arounds, and other important deployment information for Red Hat Certificate System 7.2.

Additional Certificate System information is provided in the Certificate System SDK, an online reference to HTTP interfaces, javadocs, samples, and tutorials related to Certificate System. A downloadable zip file of this material is available for user interaction with the tutorials.

For the latest information about Red Hat Certificate System, including current release notes, complete product documentation, technical notes, and deployment information, see *http://1www.redhat.com/1docs/1manuals/1cert-system/*.

9. Copyright and Third-Party Acknowledgments

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.2 servers include the following:

Apache Software Foundation

Red Hat Certificate System TPS subsystems require a locally-installed Apache 2.0.x HTTP server. Although a local copy of this server is generally installed as part of the operating system (with its corresponding license located in **/usr/share/doc/***httpd-version***/LICENSE**, the latest version of this server is available at the following URL:

http://1httpd.apache.org

Red Hat Certificate System CA, DRM, OCSP, and TKS subsystems use a locally-installed Tomcat 5.5 web server. Although an appropriate server is installed when any of these subsystems are installed, the latest version of this server is available at the following URL:

http://1tomcat.apache.org

Red Hat Certificate System uses many components made available from Apache.

- The XML project jars are **crimson.jar** and **xalan.jar**. These are available at the following URL:

  http://1xml.apache.org

- The Tomcat project jar files are **servlet.jar** and **jakarta-naming.jar**. These are available at the following URL:

  http://1jakarta.apache.org/1tomcat/1index.html

Mozilla Foundation

Red Hat Certificate System uses version 4.2 of the Java™ Security Services (JSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of and, potentially, the binary images for newer versions are available at the following URL:

http://1www.mozilla.org/1projects/1security/1pki/1jss/1index.html

Red Hat Certificate System also uses version 4.6 of the Netscape Portable Runtime (NSPR) lib-

raries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

http://1www.mozilla.org/1projects/1nspr/1index.html

Additionally, Red Hat Certificate System uses version 3.11 of the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

http://1www.mozilla.org/1projects/1security/1pki/1nss/1index.html

Red Hat Certificate System includes a set of compiled binaries (from NSS 3.11) of several tools from the Mozilla Project provided for the convenience of the user. This includes **`certutil`**, **`cmsutil`**, **`modutil`**, **`pk12util`**, **`signtool`**, **`signver`**, and **`ssltap`**. If any problems are found in these specific tools, the source code and build instructions for the latest version of this tool and, potentially, a binary image for other newer tools are available at the following URL:

http://1www.mozilla.org/1projects/1security/1pki/1nss/1tools/1index.html

Red Hat Certificate System includes version 1.5 R3 of Rhino JavaScript for Java™. If any problems are found in this specific distribution, the source code and build instructions for the latest version and, potentially, a binary image are available at the following URL:

http://1www.mozilla.org/1rhino/1index.html

Red Hat

Red Hat Certificate System requires a complete Red Hat Directory Server 7.1 binary, and the open source portion of Certificate System is available at the following URL:

https://1rhn.redhat.com

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.2 clients include the following:

Mozilla Foundation

USE AND AVAILABILITY OF OPEN SOURCE CODE. Portions of the Product were created using source code governed by the Mozilla Public License (MPL). The source code for the portions of the Product governed by the MPL is available from *http://1www.mozilla.org* under those licenses.

Red Hat Enterprise Security Client uses the latest version of the XULRunner cross-platform package. XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. If any problems are found in this specific distribution, the source code and build instructions for the latest versions and, potentially, a binary image are available at the following URL:

http://1developer.mozilla.org/1en/1docs/1XULRunner_1.8.0.1_Release_Notes

Red Hat Enterprise Security Client also uses the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

http://1www.mozilla.org/1projects/1nspr/1index.html

Red Hat Enterprise Security Client also uses the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

http://1www.mozilla.org/1projects/1security/1pki/1nss/1index.html

Additional Red Hat Enterprise Security Client smart card libraries and modules:

- e-gate Smart Card Drivers for Windows 2000/XP Copyright 2002-2003 Schlumberger. All rights reserved.

- e-gate Smart Card Driver for Mac OS X Copyright 2003 by Chaskiel Grundman.

  Copyright 2003 by Philip Edelbrock.

  Significantly based on the Alladin etoken driver (the T=1 code is not needed): Copyright 2002 by Andreas Jellinghaus.

  Copyright 2002 by Olaf Kirch.

  See license terms below for rights on both parts.

  Some header files are from the pcsclite distribution: Copyright 1999 David Corcoran.

- MUSCLE smart card middleware and applets

  Copyright 1999-2002 David Corcoran.

  Copyright 2002 Schlumberger Network Solution.

  All rights reserved.

The following license terms govern the identified modules and libraries:

- e-gate Smart Card Drivers for Windows 2000/XP:

  Limited Warranty/ Exclusive Remedies. Schlumberger warrants to the benefit of Customer only, for a term of sixty (60) days from the date of acquisition of the e-gate Smart Card ("Warranty Term"), that if operated as directed under normal use and service, the Software will substantially perform the functions described in its applicable documentation. Schlumberger does not warrant that the Software will meet Customer's requirements or will operate in combinations that Customer may select for use, or that the operation of the Software will be uninterrupted or error-free, or that all Software errors will be corrected. Schlumberger's sole obligation and liability under this limited warranty shall be, at Schlumberger's option, to remedy any substantial non-performance of the Software to the functional descriptions set forth in its applicable documentation. If Schlumberger is unable to satisfy the foregoing limited warranty obligations during the Warranty Term, then Schlumberger shall, upon Customer's written request for termination of this Agreement, refund to Customer all sums paid to Schlumberger for the licensing of the Software hereunder. These are Customer's sole and exclusive

remedies for any breach of warranty.

WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 5 ABOVE, THE SOFTWARE IS PROVIDED AS IS. SCHLUMBERGER AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES. TO THE EXTENT AUTHORIZED BY APPLICABLE LAW, ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, ARE SPECIFICALLY DISCLAIMED. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT.

Limitation of Liability. Schlumberger's cumulative liability to Customer, or any third party, for loss or damages resulting from any claim, demand or action arising out of or relating to this Agreement or use of the Software (''Damages''), shall not exceed the net amount paid to Schlumberger for the licensing of the Software, in this case, the cost of the single e-gate Smart Card. In no event shall Schlumberger or any Supplier be liable for any indirect, incidental, special consequential or exemplary damages of any character, including, without limitation, damages for lost profits, goodwill, work stoppage, computer failure and all other commercial damages.

- e-gate Smart Card Driver for Mac OS X:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

  - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

  - The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- MUSCLE smart card middleware and applets:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  1. Redistributions of source code must retain the above copyright notice, this list of conditions and

the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

10. Document History

Revision History

Revision 7.2.1	January 14, 2009	Ella Deon Lackey dlackey@redhat.com

Updated release information, per Errata RHSA-2009:0006.

Revision 7.2.0	December 8, 2006	Ella Deon Lackey dlackey@redhat.com

Initial release.